Blockchain And Deep Learning for Preventing Cyberstalking and Online Harassment of Women

A Synopsis

Submitted in

Partial Fulfilment for the Degree

Of

Doctor of Philosophy

(Computer Science)

Supervised by:

Dr. Raj Sinha,
Assistant Professor,
School of Computer Applications,
Lovely Professional University,
Jalandhar, Punjab

Submitted by

JV'nMahesh Narayan Sharma

Enrolmentno.JVR-JVR-II/21/5907

Department of Computer Science

Faculty of Management & Humanities

JayotiVidyapeethWomen'sUniversity

Jaipur (Rajasthan), India

2024

Abstract

The web, more than ever, has become the ground that harbors cyberstalking, among others, against women. Along with these, various other manners of online harassment have become the centerpiece ofthecriticalsocialissuesofthisdigitalage.Thesebringsignificantthreatstothementalhealth and security of an individual, ultimately bearing the damages on well-being at large. The existing approach used to counter these has been found in most cases inadequate and too late, besides being anonymous in nature. This paper outlines a new framework, synergizing Blockchain technologywith Deep Learning, in order to enhance online harassment detection while preventing it. We aspire here towards the creation of a proactive system that safeguards users from cyberspace threats by making use of the immutability and decentralization of blockchain, and the advanced capabilities of deep learning algorithms. This system employs cutting-edge deep learning techniques that include, withoutlimitations,CNNsandRNNs,withaspecialfocusonusingLSTMforsequencepredictions. These models will be utilized both in sentiment analysis and in the discovery of abusive language patterns in the textual communications: We also employ NLP tools like BERT, that has shown promise in the context of understanding nuances in language, toward the determination of a message's intent as either harmless or harmful. Towards security improvement we recommend that the blockchain must be formed using the hash of graphical images, so evidence related toharassment is forever tamper-proof. Thus, this method will authenticate the genuineness of theimage without revealing the images and thereby keep the victims' identity anonymous while the evidence is legitimate. Additionally, we will deal with the implementation of Zero-Knowledge Proofs (ZKPs) that allow the proof of statements without disclosure of sensitive information. Smart contracts will also automate operations in the following manner: Automatically warn users, imposea temporary restriction or even push such cases to authorities for further investigation.Through wide-scaledataacquisitionfromtheinternet,coupledwithdevelopmentofdeeplearningmodels,

we will be able to test its performance in real-time scenarios. The expected outcomes are a robust automated system that alerts the users and the authorities and logs the incidents in a tamper-proof manner, thus enhancing accountability and encouraging victims to come forward.This research aims to put together a foundation for a safer digital space while enabling women and other vulnerable groups to defend themselves against digital threats. We tap the potential of blockchain as well as deep learning to contribute to both technological innovation and discourse for online safety.

Introduction

The internet has really transformed the face of communication-it has brought people from all walks of life within each other's arms. It facilitates connections across geographical boundaries and brings about the exchange of ideas and information [1]. But thisincreased connectivity has also given birth to a most disturbing phenomenon: cyberstalking and online harassment. Cyberspace stalking refers to the continuous, unwanted surveillance or harassment of an individual through digital media, which often includes repeated messages and threats or even invasive surveillance of a person'sonline activities. Such abuse becomes a personal boundary violation to the victims and equally makes the victims vulnerable to and afraid of being victimized at any one time. On the contrary, onlineharassment takes avariety ofnegativeactivitiesthat comein different forms in thespheres of cyberbullying, hate speech and abuse of disseminating private information. Among both men and women, these hostile activities are known, but women tend to seriously suffer from online harassment as well as cyberstalking [1].

Cyberstalking and online harassment have reached alarming statistics against women, and this is now an important issue in modern society. A recent study shows that nearly 25% of women experience some type of harassment online, which number is particularly higher among young women and minorities. This dangerous trend can be further sustained with the anonymity digital platforms often provide, making perpetrators bold enough to act out with impunity. Cyber interactions by definition enable harassers to hide behind masks, even making it considerably challenging for victims to take recourse measures [2].

Under such circumstances, many women are helplessly trapped into spiralling cycles of abuse and feelunabletoprotectthemselvesorevenknowwhomtoturntoforprotectionagainstthisreality.

There are implications of cyber stalking and online harassment that have far-reaching consequences beyond immediate emotional distress to risk the very existence of women. Significant psychological effectsthathavebeenreportedbythevictimsincludehigherlevelsofanxietyanddepression,andin extreme cases, post-traumatic stress disorder [2]. The emotional impact can lead to far-reaching feelings of alienation and fear, as victims may change their online behaviours, reduce the scope of social interactions, or even withdraw from digital spaces. This withdrawal affects not only their private and professional lives but also curtails freedom of expression and engagement in online communities. These changes are disastrous especially in an increasingly digital communication world for socializing, education, and business [3].

While cyberstalking and online harassment have gained in prominence, existing solutions fail tohelp fill the gap. Currentsolutions offer mainly a reactive approach rather than preventive solutions, relying instead on user-reported incidents and content moderation. As such, while these approaches can offer some form of response, they are by default hamstrung by the delays in action and the inconsistenciesofenforcement.Moreover,decentralizationremainsaproblemconcerningtheonline space since perpetrators can easily be eluded or even change identities. This, in turn, leaves the victim very helpless and unsupported; such is the need for stronger proactive measures towards guaranteeing their safety in digital space [3].

Thus, in light of such problems, there is a critical and urgent need for new technological solutions capableofeffectivelyfightingcyberstalkingandonlineharassment. Itisjust thisuniqueopportunity that blockchain technology presents in terms of creating a fully decentralized, transparent, andsecure environment for the management of harassment evidence. By employing blockchain technology in the system, harassment reports can be ensured to be stored in a tamper-proof way whiletheintegrityandconfidentialityofinformationrelatedtovictimsaremaintained.Thus,Deep

Learningalgorithmsareintegratedintothissystemandaresoincorporatedtoprovidepowerful real- time analysis tools for online interactions, such as techniques for detecting patterns of abusive behaviour, thus possible earlier identification of potential threats before they escalate through the applications of Natural Language Processing and Machine Learning [4].

Combining these leading-edge technologies, this research aims at developing an integrative framework that not only improves detection and prevention capabilities for cyberstalking and online harassment but also empowers women to take control of their online space. The proposed system will employ the hash of graphical images in preserving the integrity of the evidence while keeping theidentitiesofthevictimssecret.Otherthingsbeingequal, smart contractscanbeused toautomate several response mechanisms, which may instantly alert users to the possible need for actions such as issuing a warning, temporarily banning them from using the platform, or escalating the incidentto law enforcement if harassment is identified. This innovation will lead us on the path to creating a safer online environment that enables open communication and protects the rights and well-being of all its citizens, especially women.

1.2 RoleofDeepLearninginPreventingCyberstalkingandOnline Harassment

DeepLearningplaysanextremelycriticalrolein preventingcyberstalkingandonlineharassmentby its use of advanced capabilities to process and analyze huge volumes of unstructured data to determine complex patterns that are indicative of harmful behaviors. Some of the other applications of deep learning have been taken up to analyze sentiment, for example, through models like BERT and LSTM networks, which assess the emotional tone of online communications. Such models can classify messages into abusive or non-abusive statuses, so the platform can intervene and preventtheharmarisingfromthosecontentsbeforetheyevergetthechancetoreachothers.Forinstance,

whenever an abusive text has been detected, immediate automated responses can alert both the user and moderators, handling the situation before it worsens [5]. Beyond text analysis, deep learning also is extremely useful for content processing that often may be represented in a visual manner. Convolutional Neural Networks (CNNs) are highly suitable for the analysis of images and videos to identify manipulated content as well as malicious content. For example, in the case of a person posting a manipulated image intended to harm another person's reputation, CNNs will detect anomalies or traces of tampering, thereby providing extra security from visual harassment. This is urgently needed today with rampant digital forms of image harassment [5].

Deep learning also has great capabilities through real-time threat detection and monitoring. These systems can be continuously scanning for signs of abusive language or patterns of harassment on social media platforms, forums, and chat rooms, providing instant alerts both to users and moderators. This proactive approach enables rapid responses to emerging threats and may even prevent escalations of harassment. Deep learning also gives a boost to automated moderation tools. They can automatically flag content based on the basis of its severity and urgency. This ensures that critical issues of harassment get dealt with, thereby reducing some of the loads on humanmoderators and increasing efficiency [5].

Another critical point where deep learning finds its place in the context of online interactions is contextual understanding. Such technology performs very well on nuances of language that may catch elements of harm as well as benign communication through systems that could identify the lack of intent in messaging. It would mean that, even with typical cues such as sarcasm or culturally exclusive references that make the interpretation of messages difficult, advanced models for natural language processing can be analyzed in a better way to provide more accurate assessments. This reallyreducesthepotentialformisinterpretationandfalsepositivesinthecontextofdealingwith

harassment. Finally, deep learning can potentially allow stalking and harassment analysis by studying the typical user interaction pattern. A model will be capable of detecting outliers that may represent stalking or harassment. For example, when the interaction pattern is in an unusual state of having many messages from the same user on someone's account, the system can raise a flag for review.Itisthroughsuchpredictiveanalyticsthatswiftinterventionbecomespossible,andusersare also empowered with insights into their safety online, thus helping take proactive measures to avoid certain situations [6].

The Deep Learning integration in the strategies to curb cyberstalking and online harassmentprovides a comprehensive approach at enhancing the detection and management of harmful behaviors. More power should be sent toward online configurations with enhanced algorithms on sentiment analysis, visual content processing, real-time monitoring, contextual understanding, and behavioral prediction to reinforce online safety. The transformative technology creates a saferdigital environment. The power to enable women and more to confidently surf the web without threats of harassment and intimidation is immense.

1.3 RoleofBlockchaininCombatingCyberstalkingandOnline Harassment

Blockchain technology, in itself, provides a secure, transparent, and decentralized framework for managing evidence of abuse. Therefore, its principal feature of creating tamper-proof records helps ensure that any report of harassment will be securely logged and cannot be destroyed or altered by malicious actors [6]. This is particularly essentialin the incidences of the victims who may notwant to offer such information because with blockchain, their evidence will not be tampered with. One could use hashing techniques where one could store graphical images concerning harassment incidentsasuniquehashesintheblockchain;thisway,oneguaranteestokeepoutthesensitivedata

but still presents verifiable evidence. Additionally, the decentralized nature of blockchain offers an open reporting mechanism that can be run single-platform free to minimize biases in reporting and also censorship. Automations toward harassment issues could be brought about through smart contracts,sendingwarningstoharassersor temporarilybanningusersdependingontheimplications and occurrence rates of incidents reported. This automation does not only make the responses much faster but also gives a uniform response towards abuses. Immutability of blockchain records further allows law enforcement to gather legally verified proof of cyberstalking and online harassment as more effective means of investigations and legal practices against the offenders. Hence, applying blockchain technology to online networking sites would allow us to ensure people are safe from harassment and abuse, thus always making a safer digital space for everyone [6].

Objectivesof the Study

Theobjectives of thestudy are:

1. To conduct a comprehensive literature review on the use of blockchain and deep learning in cybersecurity and online harassment prevention.
2. To develop a blockchain-based system for securely storing and managing evidence through the hashing of graphical images.
3. To design and implement deep learning models for real-time detection of abusive text andvisual content.
4. Toenhancedetectionaccuracybyintegratingsentimentanalysisandbehavioralpattern recognition techniques.
5. Tocreateautomatedalertsandinterventionsusingsmartcontractsforfasterresponsesto harassment incidents.
6. Toevaluatetheeffectivenessoftheproposedframeworkinimprovingusersafetyand reducing online harassment.

LiteratureReview

Wen, B., et al. (2023) [7]: Blockchain technology has become essential across multiple domains, including digital currency, IoT, smart grids, and finance. However, its adoption presents challenges in privacy and security. This paper provides an overview of blockchain applications, focusing on privacy protection, security supervision, and data exchange, while discussing future research directions.

Thakur, G., et al. (2023) [8]: Digital Twin (DT) technology, used in healthcare, manufacturing,and aerospace, faces security vulnerabilities. This study critiques a two-factor blockchain-based authentication protocol for DT environments, exposing its weaknesses. To address these issues, the authors propose a more secure three-factor authentication scheme, validated using Burrows-Abadi-Needham (BAN) logic and the Real-or-Random (ROR) model.

Chentouf, F. Z., & Bouchkaren, S. (2023) [9]: This paper explores blockchain applications within smart cities, driven by IoT integration. It discusses how blockchain features—transparency, decentralization, and security—can enhance urban services. An Ethereum-based smart contract voting model is introduced to showcase blockchain's potential for secure smart city operations.

Sultan, D., et al. (2023) [10]: With social media's expansion, cyberbullying has become a pressing issue. This study evaluates shallow and deep learning methods for detecting cyberbullying. Results demonstrate that Bidirectional LSTM achieves the highest accuracy and recall, making it the most effective method for identifying online harassment.

Marshan, A., et al. (2023) [11]: This research investigates the severity of abusive comments on socialmedia.ItcomparesmodelssuchasNaïveBayes,RandomForest,andCNN.TheRandom

Forest with bigrams achieves superior performance with an accuracy of 94%, along with high precision, recall, and F1 scores, making it ideal for detecting severe abusive behavior.

Islam, M. S., et al. (2024) [12]: This paper proposes a machine learning framework to detect cyberbullying using advanced NLP techniques, including text preprocessing, feature extraction, and sentiment analysis. The results indicate that SVM is the most effective model with a 90.06% accuracy rate, making it a reliable tool for online safety.

Amer, N., & Dhannoon, B. N. (2023) [13]: This study addresses early detection of sexual harassment using machine learning models like SVM, Logistic Regression, and XGBoost. The research, using Chats Sexual Predators (CSP) and Comments Sexual Harassment (CSH) datasets, achieved high accuracy, with Logistic Regression reaching 98.44%. XGBoost demonstrated resilience against overfitting, yielding promising results across both datasets.

Alawneh, E., et al(2021)[14] : Cyberbullying and sexual harassment are examples of these bad online actions that impact not only legitimate users but also governments and others involved. This research improves the design of machine learning classifiers to detect and classify such malicious activities more effectively. The experiments determined that Term Frequency Inverse Document Frequency used together with algorithms in machine learning yields an accuracy rate of 81%.

Espinoza, I., & Weiss, F. (2020) [15]: discuss the persistence of online harassment since the inception of social networks, emphasizing its serious implications for victims based on factors such as gender, race, and sexuality. They note that existing automated systems designed to detect and report harassment often struggle to generalize across different data types. The authors introduce a newdatasetforharassmentdetectiononTwitter,whichcontainsfourclasses,createdforthe

SIMAH competition. They applied three deep learning architectures—CNN, LSTM, and BiGRU—to classify the tweets, revealing the challenges posed by limited annotated data. Their results achieved a maximum f1-score of 46% on the test set and 55% when using all available data for training.

Table1.LiteratureReviewonLexiconApproaches

Author Name (Year)	**Main Concept**	**Findings**
Wen, B., et al. (2023)	Overviewofblockchainapplications	Discussesprivacyprotection,security supervision, and data exchange in blockchain;highlightsfutureresearch directions.
Thakur,G.,etal. (2023)	DigitalTwin(DT)technologyand authentication	Proposes a secure three-factor authentication scheme for DT environments, addressing vulnerabilitiesinexistingprotocols.
Chentouf,F.Z.,& Bouchkaren, S. (2023)	Blockchaininsmartcities	Explores how blockchain features enhance urban services; presents a smartcontractvotingmodelon Ethereum.
Sultan,D.,etal. (2023)	Detection of cyberbullying using machine learning	FindsBidirectionalLSTMtobethe mosteffectivemethodfordetecting cyberbullying,withhighaccuracy

		andrecall.
Marshan,A.,etal. (2023)	Severity detection of abusive comments on social media	Demonstrates Random Forest with bigrams achieves 94% accuracy, high precision,andrecallfordetecting severe abuse.
Islam,M.S.,etal. (2024)	Cyberbullying detection using machine learning	Shows SVM as the most effective algorithm with 90.06% accuracy, improvingonlinesafetythrough advancedNLPtechniques.
Amer, N., &Dhann oon,B.N. (2023)	Earlydetectionofsexualharassment using machine learning	Logistic Regression achieves 98.44% accuracy; XGBoosteffectivelyavoids overfittingacross datasets.
Alawneh,E.,etal. (2021)	Proposing a machine learning approachtoenhancedetectionand classification of malicious human activities in cyberspace.	Achievedanaccuracyrateof81%by combining TF-IDF with machine learning algorithms.
Espinoza, I., & Weiss,F.(2020)	Addressingonlineharassmentandits impact on victims, with a focus on creatinganewdatasetforharassment detection on Twitter.	Achieved a maximum f1-score of 46% on the test set and 55% when usingallavailabledatafortraining.

Basedontheliteraturereviewed,thefollowingresearchgapscanbeidentified

1. **Security Vulnerabilities**: Existing authentication protocols, especially in Digital Twin environments and blockchain applications, often have unresolved security weaknesses that need further investigation.

2. **Integration of Technologies**: There's a need for more comprehensive approaches that combine multiple technologies (e.g., machine learning and blockchain) to enhance security and privacy in applications like smart cities and healthcare.

3. **GeneralizabilityofModels**:Manymachinelearningmodelsfordetectingcyberbullyingand harassment are often trained on specific datasets, which may not generalize well across different platforms or languages.

4. **User-Centric Approaches**: Research often lacks a focus on user experiences and perspectives when designing systems for detecting online abuse, indicating a need for more user-centered studies.

5. **Lack of Standardization**: The absence of standardized protocols and frameworks for implementing blockchain and machine learning technologies limits their widespread adoption and interoperability.

StatementoftheResearchProblem

Cyberstalkingandonlineharassmenthave,however,becomerampantproblemsinthedigitalage and tend to affect more women and other vulnerable groups. Taking advantage of the explosion in social media, messaging applications, and online communities, harassers have learned to exploit these channels to stalk, intimidate, or threaten others. Most of the current measures todeal with these deviant behaviors continue to rely heavily on content moderation and reporting mechanismsthatarereactionaryandcanbearbitraryandbiased.Thesetraditionalsystemsfailto handle such a vast number of online interactions and often miss subtle or context-dependent forms of harassment. Furthermore, many victims cannot readily collect credible evidence and ensure their complaints will be taken seriously by the platforms and law enforcement agencies. But in all this, an important question arises: how can real-time actual harmful behavior be detected? with effective solutions and keeping the privacy of users? How can evidence be managed safely and securely so as to avoid risks of tampering or deletion? How can trust be established between platforms, users and law enforcement agencies for swift and unbiased action?

This researc will therefore find answers to the above challenges by proposing a novel framework thatintegrates blockchaintechnology anddeeplearningalgorithmsforpreventingandmitigating cyberstalking and online harassment. Specifically, blockchain will be utilized in establishing an immutable, decentralized record-keeping system storing hashes of graphical images as evidence of security and transparence. The real-time analysis of textual and visual content is expected to detect patterns of abusive behavior and nuanced context, sentiment, and behavioral patterns with the aid of deep learning models. The proposed technology hopes to bridge the three gaps: security,user safety,and technology,whileit offersproactive andscalable mitigationofthe risks

involved in online harassment. The outcome will free platforms to react promptly and with definiteness, offering victims sure mechanisms for reporting abuse, offering protection for their evidence, and accountability at all levels.

Research Methodology

This research will follow a systematic approach that combines blockchain technology and deep learning models to develop a robust framework for preventing cyberstalking and online harassment. The methodology will be divided into several phases, focusing on data collection, model design, blockchain integration, and evaluation.

1. **Literature Review:** A detailed review of existing research on cyberstalking, online harassment, blockchain applications in cybersecurity, and deep learning-based threat detection will be conducted. This phase will identify gaps in existing systems and helpdesign a framework that addresses those limitations.

2. **DataCollectionandPreprocessing:**

    - **Textual Data:** Publicly available datasets, such as Twitter or online forum data containing abusive and non-abusive content, will be gathered.

    - **Image and Video Data:** Datasets containing manipulated or harmful media relevant to harassment will be used for training visual detection models.

    - **Survey Data:** A survey will be conducted to collect qualitative and quantitative data on women's experiences with cyberstalking and online harassment. This survey aims to gather insights into the prevalence, impact, and forms of harassment faced, informing the design and refinement of the framework.

    - Data will be cleaned, labelled, and pre-processed to ensure consistent input for the deep learning algorithms.

3. **DesignandDevelopmentofDeepLearningModels:**
    - **TextAnalysis:**SentimentanalysismodelsusingLSTM,BERT,orTransformer- based architectures will be trained to detect harmful language.
    - **ImageandVideoAnalysis:**CNN-basedmodelswillidentifyoffensiveor manipulated visual content used for harassment.
    - **BehaviourAnalysis:**Anomalydetectionmodelswillmonitoruseractivitytoflag suspicious behaviours indicative of stalking.
4. **Blockchain Integration:**
    - A blockchain ledger will be designed to store hashes of evidence (text, images, andvideos), ensuring data security and integrity.
    - Smart contracts will automate interventions, such as triggering warnings or reporting incidents to moderators based on the severity of the harassment.
    - Decentralizationwillensurethatevidenceistamper-proofandaccessibletoauthorized stakeholders, such as law enforcement.
5. **SystemDevelopmentand Implementation:**
    - The deep learning models will be integrated into a real-time monitoring system, with alerts triggered based on detected threats.
    - Theblockchainmodulewillinteractwiththedetectionmodelstologevidencesecurely.

6. **Testingand Evaluation:**

    - Thesystemwillbetestedusingreal-worldscenariosanddatasetstoevaluateits accuracy, speed, and reliability.
    - Performance metrics such as precision, recall, F1-score, and detection time will beanalyzed.
    - Acomparativeanalysiswillbeconductedwithexistingonlineharassmentprevention systems to demonstrate the effectiveness of the proposed solution.

7. **Feedbackand Refinement:**

    - Based on the evaluation results and stakeholder feedback, the system will be refined to improve its performance and scalability.

This research methodology ensures a comprehensive approach, addressing both the technical and social challenges involved in preventing cyberstalking and online harassment. By incorporating survey data alongside technical implementations, the research aims to provide victims with reliable tools for protection and reporting, while also contributing valuable insights to inform future developments in the field.

Dataset

The dataset used in this research will comprise a variety of sources to ensure a comprehensive analysis of cyberstalking and online harassment. Publicly available datasets, such as those from Twitter and online forums, will be collected to gather textual data containing both abusive and non-abusive content. Additionally, image and video datasets that include manipulated or harmful media relevanttoharassmentwillbeemployedfortrainingvisualdetectionmodels.Toenhancethe

robustness of the dataset, we will also utilize curated datasets from Kaggle, which offer diverse examples of online harassment and abusive language patterns. Furthermore, a survey will be conducted to collect qualitative and quantitative data on women's experiences with cyberstalkingand harassment, providing valuable insights to complement the existing datasets. This multi-faceted approach ensures that the dataset is rich and varied, allowing for effective training and evaluation of the deep learning models developed in this research.

PrimaryData

Primary data for this research will be gathered directly through a survey in order to build an understanding of the experiences of women with cyberstalking and online harassment. Both qualitative and quantitative questions will be used in the survey so that prevalence, forms, and psychological impact of such harassment could be captured. It will also give insights into user awareness regarding the measures in place for online safety, mechanisms for reporting, and their effectiveness. This primary data will thereforebe useful in providing critical insights to patterns and intensity of online abuse, victim behavior, and gaps in the current system of prevention. The responses would be critical in tailoring the proposed blockchain and deep learning framework to respond to real-world issues. Because primary data are collected, the solution is going to reflect the needs and experiences of the affected demographic, thus allowing development of more targeted intervention strategies.

SecondaryData Sources

Secondary data will be derived from public and curated datasets, such as social media datasets from Twitter and online forums, and derived from Kaggle. These would include both abusive and non-abusivetext,aswellasimagesandvideorecordingsthatcouldhavebeenusedincasesofonline

harassment. Secondary data would be preprocessed before its utilization in the training of deep learning models used in the analysis of text sentiment, the detection of offending content, and the discovery of behavioural anomalies. A literature review of earlier literature on cyberstalking, harassment, blockchain applications in cybersecurity, and deep learning techniques would supplement secondary data. In addition, this extensive use of secondary data will also furthersupport the training process for the models. The results can further be applied as a comparative benchmark to assess whether the proposed framework does indeed work or not.

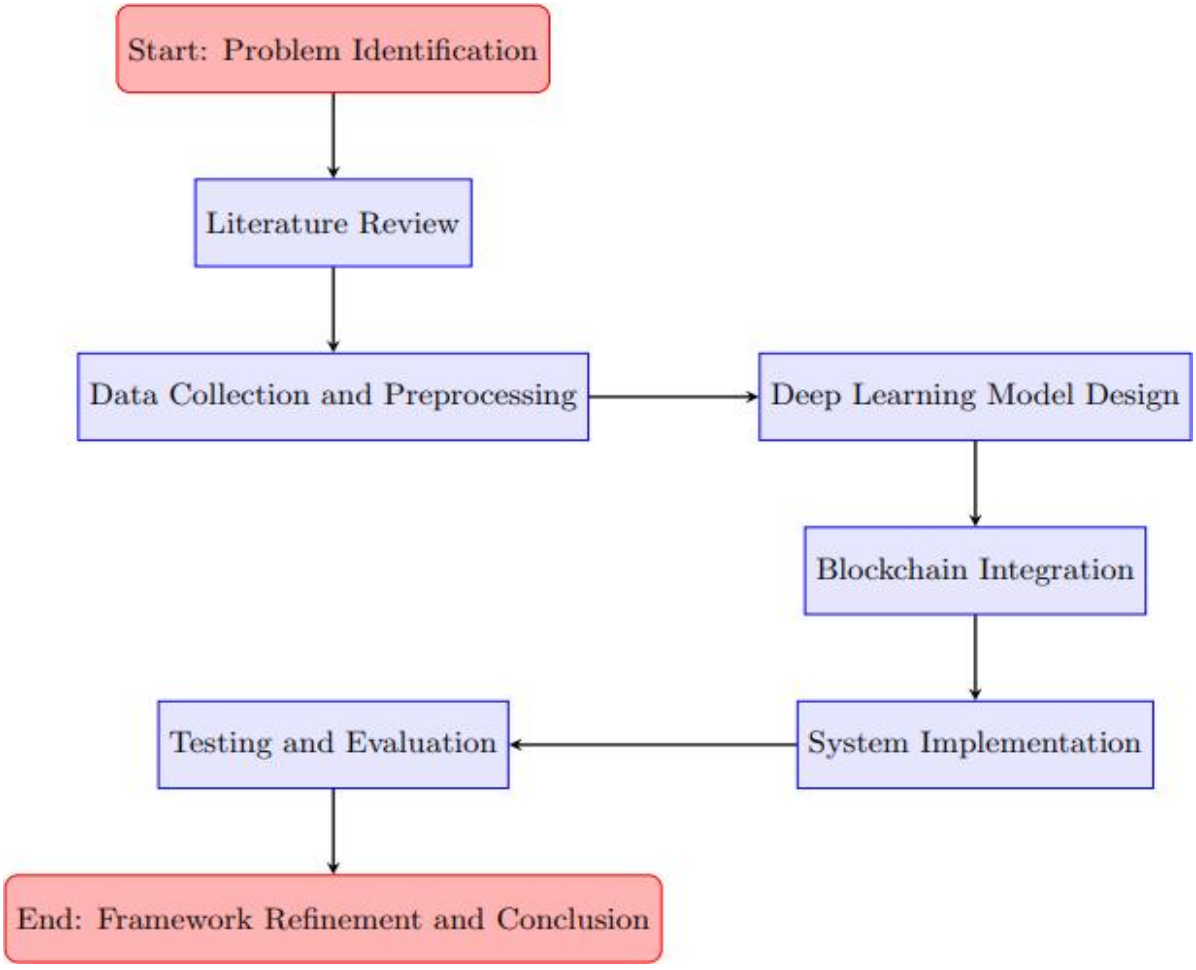

Figure1.ResearchFlowDiagram

Statisticaltoolsandmethods

Statistical analysis will be applied to the collected data through the actual conducting of surveysand other secondary sources to give meaningful inferences. Microsoft Excel will be applied as the main tool for the entering, organizing, and analysis of data. Descriptive statistics such as mean, median, mode, and standard deviation will be calculated to sum up the distribution and central tendencies of the collected data. The frequency distributions and cross-tabulations will identify trends such as the most common types of abuse, age groups, and frequency of reporting.

AlgorithmsUsed

- **Long Short Term Memory (LSTM) :** Long Short-Term Memory, or LSTM networks, for that matter, are a special type of recurrent neural network that is defined to learn from sequences over long time intervals. LSTMs operate around the problem of vanishing gradients that occurs often in standard RNNs, thus they can remember information over many time steps. This feature makes LSTMs perfectly suited for tasks such as time series prediction, language modeling, and sentiment analysis tasks, where the information about previous inputs has to be known before making the best possible predictions. This happens because of the special architecture with memory cells and input/output/forgetting gates through which they can control the flow of information, keeping what is important from the past and filtering out irrelevant data. This is the ability to handle long-range dependencies which makes LSTMs powerful in NLP as well as other sequence-based applications.
- **Bidirectional EncoderRepresentations from Transformers (BERT):**BERT is an open-source pre-trained model by Google, and it is one of the most acclaimed state-of-the-art modelsfornaturallanguageprocessing.BERTusestransformerarchitecturetofacilitate

textin bothdirections: left-to-rightandright-to-left simultaneously.Thistwo-wayapproach enables BERT to contextualize the meaning of words in terms of surrounding words more effectively than other unidirectional models. BERT is trained on large corpora with unsupervised learning techniques, in which it learns to predict missing words in sentences, which gives a deep understanding of the nuances and syntax of language along with semantics. Due to its high accuracy and ability to generalize across different datasets,BERT has had widespread applications over various NLP tasks, such as sentiment analysis, question answering, and named entity recognition.

- **Convolutional Neural Network (CNN) :** Convolutional neural networks (CNNs) are a family of deep learning algorithms that have been specifically optimized for structured grid data, like images. Being based on the principles of the convolution involved in applying filters to the input data to extract hierarchical features automatically, CNN architecture involves several layers like convolutional, pooling, and fully connected layers, all allowinga model to progressively learn increasingly complex representations of the input data.CNNs are superior in image-classification tasks, object detection and detection tasks ofsuch other visual activities where the spatial hierarchies and patterns can be captured effectively. Especially they are strong features in identifying structures, textures, andobjectsinsideimages,makingthemreallyusefulforareaslikecomputervisionandmedical imaging. The possibility of reducing parameters by weight sharing and local connectivity makes CNNs computationally efficient and suitable for handling large datasets.

- **RecurrentNeuralNetwork(RNN)**

  Recurrent Neural Networks are a class of artificial neural networks designed for processing sequentialdatabyretainingtheinformationofwhathappenedinearliertimesteps.RNNs

areespecially useful for tasks that involve processing with temporal or ordered data. Unlike traditionalneuralnetworks,thehiddenstatesofRNNhaveconnectionsthatareloopedback to store information coming from earlier inputs. This makes RNNs capture the dependency between elements in a sequence, such as words in a sentence or time series data-things very important for tasks like language modeling, speech recognition, and sentiment analysis.

However, standard RNNs suffer from the vanishing gradient problem, that is, an issue with learning long-term dependencies because gradients become too small to update the weights effectively over a significant number of time steps. Examples of such variants include LSTM networks and Gated Recurrent Units, which try to solve the problem by allocating memory cells with gates to regulate the flow of information. In this study, RNNs will be applied in examining sequential patterns of user behavior and text data, which can be used for identifying suspicious activities related to cyberstalking and harassment.

HypothesesfortheResearchStudy

1. Primary Hypothesis (H1): Integrating blockchain technology with deep learning models significantly enhances the detection and prevention of cyberstalking and onlineharassment of women by providing tamper-proof evidence storage and automated threat detection.

2. NullHypothesis(H0):Thereisnosignificantimprovementinthedetectionandprevention of cyberstalking and online harassment through the integration of blockchain and deep learning compared to existing approaches.

ProposedOutcomes

- The blockchain-based system provides the evidence about harassment in a secure manner and cannot be altered or deleted. Hence, it will have reliable evidence in the hands of victims and authorities as well.
- With the implementation of deep learning models, the system would detect cyberstalking and abusive content with real-time inputs and take immediate remedial measures.
- Thesmartcontractswillautomaticallyperformactslikeissuingwarningsorsubmissionof reports without bias and in a timely manner so that no delay is experienced during case handling.
- The system will empower victims with a safe and reliable environment to report incidents, keep evidence, and receive support in time from platforms or law enforcement.
- This will help integrate the solution across social media and other communication platforms to work toward safety online for women and vulnerable users.

REFERENCES

1. Hasan, M. T., Hossain, M. A. E., Mukta, M. S. H., Akter, A., Ahmed, M., & Islam, S. (2023). A review on deep-learning-based cyberbullying detection.*Future Internet*,*15*(5), 179.
2. Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L., & Hardjono, T. (2024, May).Sok:Securityand privacyofblockchaininteroperability.In *2024 IEEESymposiumon Security and Privacy (SP)* (pp. 3840-3865). IEEE.
3. Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges andfuture trends. *Electronics*, *12*(3), 546.
4. Sultan, D., Omarov, B., Kozhamkulova, Z., Kazbekova, G., Alimzhanova, L., Dautbayeva, A., ... & Abdrakhmanov, R. (2023). A Review of Machine Learning Techniques in Cyberbullying Detection. *Computers, Materials & Continua*, *74*(3).
5. Kumari, V., Memon, K., Aslam, B., & Chowdhry, B. S. (2023, May). An effective approach for violence detection using deep learning and natural language processing. In *2023 7th International Multi-Topic ICT Conference (IMTIC)* (pp. 1-8). IEEE.
6. Alabdulwahab, A., Haq, M. A., & Alshehri, M. (2023). Cyberbullying Detection using MachineLearningandDeepLearning.*International Journal of AdvancedComputerScience and Applications*, *14*(10).
7. Wen, B., Wang, Y., Ding, Y., Zheng, H., Qin, B., & Yang, C. (2023). Security and privacy protection technologies in securing blockchain applications. *Information Sciences*,*645*, 119322.

8. Thakur, G., Kumar, P., Jangirala, S., Das, A. K., & Park, Y. (2023). An effective privacy-preservingblockchain-assistedsecurityprotocolforcloud-baseddigitaltwinenvironment. *IEEE Access*, *11*, 26877-26892.
9. Chentouf, F. Z., & Bouchkaren, S. (2023). Security and privacy in smart city: a secure e-voting system based on blockchain. *International Journal of Electrical and Computer Engineering*, *13*(2), 1848.
10. Sultan, D., Toktarova, A., Zhumadillayeva, A., Aldeshov, S., Mussiraliyeva, S., Beissenova, G., ... & Imanbayeva, A. (2023). Cyberbullying-related hate speech detection using shallow-to-deep learning. *Computers, Materials & Continua*, *74*(1), 2115-2131.
11. Marshan, A., Nizar, F. N. M., Ioannou, A., & Spanaki, K. (2023). Comparing Machine Learning and Deep Learning Techniques for Text Analytics: Detecting the Severity of Hate Comments Online. *Information Systems Frontiers*, 1-19.
12. Islam, M. S., Orno, A. N., & Arifuzzaman, M. (2024). Approach to Social Media Cyberbullying and Harassment Detection Using Advanced Machine Learning. *Available at SSRN 4705261*.
13. Amer, N., & Dhannoon, B. N. (2023, February). Machine learning approaches to detect online harassment using bag of words. In *AIP Conference Proceedings* (Vol. 2457, No. 1). AIP Publishing.
14. Alawneh, E., Al-Fawa'reh, M., Jafar, M. T., & Al Fayoumi, M. (2021, June). Sentiment analysis-based sexual harassment detection using machine learning techniques. In *2021 international symposium on electronics and smart devices (ISESD)* (pp. 1-6). IEEE.
15. Espinoza, I., & Weiss, F. (2020). Detection of harassment on twitter with deep learning techniques.In*MachineLearningandKnowledgeDiscoveryinDatabases:International*

WorkshopsofECMLPKDD2019,Würzburg,Germany,September16–20,2019, Proceedings, Part II (pp. 307-313). Springer International Publishing.